Amendment to the Claims

The present listing of claims is as follows:

1-9. (Cancelled)

10. (Currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

generating a client message at the client;

retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship, the embedded client private key being associated with a client public key generated and stored exclusively outside the client;

encrypting the client message with the embedded server public key; ~~and~~

sending the client message to the server;

receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion; and

authenticating the first portion of the application code with the embedded server public key.

11. (Previously presented) The method of claim 10 further comprising:

retrieving client authentication data;

retrieving the embedded client private key from a read-only memory structure in an article of manufacture in the client;

encrypting the client authentication data with the embedded client private key; and

storing the encrypted client authentication data in the client message.

12. (Original) The method of claim 11 further comprising:

retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and

storing a copy of the embedded client serial number in the client message.

13-15. (Cancelled)

16. (Currently amended) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:

instructions for generating a client message at the client;

instructions for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship, the embedded client private key being associated with a client public key generated and stored exclusively outside the client;

instructions for encrypting the client message with the embedded server public key; ~~and~~

instructions for sending the client message to the server;

instructions for receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion; and

instructions for authenticating the first portion of the application code with the embedded server public key.

17. (Previously presented) The computer program product of claim 16 further comprising:

instructions for retrieving client authentication data;

instructions for retrieving the embedded client private key from a read-only memory structure in an article of manufacture in the client;

instructions for encrypting the client authentication data with the embedded client private key; and

instructions for storing the encrypted client authentication data in the client message.

18. (Original) The computer program product of claim 17 further comprising:

instructions for retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and

instructions for storing a copy of the embedded client serial number in the client message.

19. (Currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

generating a server message at the server, the server message including application code having a first portion encrypted with a server private key and a second portion, the first portion being authenticable with a server public key;

retrieving information that was requested by the client;

storing the retrieved information in the server message;

retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is generated and stored exclusively outside the client;

encrypting the server message with the client public key; and

sending the server message to the client.

20. (Currently amended) The method of claim 19 further comprising:

retrieving server authentication data;

retrieving ~~a~~ the server private key;

encrypting the server authentication data with the server private key; and

storing the encrypted server authentication data in the server message.

21. (Cancelled)

22. (Cancelled)

23. (Currently amended) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:

instructions for generating a server message at the server, the server message including application code having a first portion encrypted with a server private key and a second portion, the first portion being authenticable with a server public key;

instructions for retrieving information that was requested by the client;

instructions for storing the retrieved information in the server message;

instructions for retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is generated and stored exclusively outside the client;

instructions for encrypting the server message with the client public key; and

instructions for sending the server message to the client.

24. (Currently amended) The computer program product of claim 23 further comprising:

instructions for retrieving server authentication data;

instructions for retrieving ~~a~~ the server private key;

instructions for encrypting the server authentication data with the server private key; and

instructions for storing the encrypted server authentication data in the server message.

25. (Currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

receiving a client message from the client;

retrieving a server private key;

decrypting the client message with the server private key;

retrieving a client serial number from the decrypted client message; ~~and~~

retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is generated and stored exclusively outside the client; and

generating a server message including application code at the server in response to the client message, the application code having a first portion encrypted with the server private key and a second portion, the first portion being authenticable with a server public key;

wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship.

26. (Original) The method of claim 25 further comprising:

retrieving encrypted client authentication data from the client message;

decrypting the client authentication data with the retrieved client public key; and

verifying the decrypted client authentication data.

27. (Cancelled)

28. (Cancelled)

29. (Currently amended) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:

instructions for receiving a client message from the client;

instructions for retrieving a server private key;

instructions for decrypting the client message with the server private key;

instructions for retrieving a client serial number from the decrypted client message; ~~and~~

instructions for retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is generated and stored exclusively outside the client; and

instructions for generating a server message including application code at the server in response to the client message, the application code having a first portion encrypted with the server private key and a second portion, the first portion being authenticable with a server public key;

wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship.

30. (Original) The computer program product of claim 29 further comprising:

instructions for retrieving encrypted client authentication data from the client message;

instructions for decrypting the client authentication data with the retrieved client public key; and

instructions for verifying the decrypted client authentication data.

31. (Currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

receiving a server message from the server, the server message including application code having a first portion encrypted with a server private key and a second portion;

retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key generated and stored exclusively outside the client; ~~and~~

decrypting the server message with the embedded client private key; and

authenticating the first portion of the application code with a server public key.

32. (Original) The method of claim 31 further comprising:

retrieving encrypted server authentication data from the server message;

retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client; and

decrypting the server authentication data with the embedded server public key; and

verifying the decrypted server authentication data.

33. (Original) The method of claim 32 further comprising:

retrieving requested information from the server message; and

in response to a determination that the decrypted server authentication data was verified, processing the requested information.

34-36. (Cancelled)

37. (Currently amended) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:

instructions for receiving a server message from the server, the server message including application code having a first portion encrypted with a server private key and a second portion;

instructions for retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key generated and stored exclusively outside the client; ~~and~~

instructions for decrypting the server message with the embedded client private key; and

instructions for authenticating the first portion of the application code with a server public key.

38. (Original) The computer program product of claim 37 further comprising:

instructions for retrieving encrypted server authentication data from the server message;

instructions for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client; and

instructions for decrypting the server authentication data with the embedded server public key; and

instructions for verifying the decrypted server authentication data.

39. (Original) The computer program product of claim 38 further comprising:

instructions for retrieving requested information from the server message; and

instructions for processing the requested information in response to a determination that the decrypted server authentication data was verified.

40. (Cancelled)